Europäisches Patentamt	European Patent Office	Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

02020471.5

Der Präsident des Europäischen Patentamts:
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 02020471.5
Demande no:

Anmeldetag:
Date of filing: 12.09.02
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

SOFTWARE AG
Uhlandstrasse 12,
Postfach 130-251
D-64297 Darmstadt
ALLEMAGNE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Signature validation and generation

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L9/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR

Software AG

September 12, 2002
S37957EP JH/Hdt/tge

Signature validation and generation

The following invention deals with methods and apparatuses for generating and validating messages with digital signatures.

If a message is sent via an untrustworthy channel, like the Internet, the content of the message and the name of the sender can be changed by not authorized persons. But the content of the message should only be stored at the receiver, when the receiver is sure about the correct sender. Electronically signed messages give the receiver the guarantee that the received message comes from the alleged person and that the message has not been changed during the transmission. The signature is information attached to the message, which is based on the content of the message and the key of the signer, for example the sender. A message can for example be signed by a value, which is the result of a common algorithm with the sender's private key over the content (or a hash) of the message. If the receiver knows the common algorithm and the public key of the sender, the receiver can apply the algorithm to the received message and compare the result with the submitted value. If the values match, the complete message originally has been sent by the owner of the key.

The generation of the signature may be carried out by a security device, which receives the content of the message in a first step, applies the algorithm with the sender's private key on the content to generate the signature and forwards the message with the signature to the receiver. The receiver comprises also a security device for the validation of the signature. If the signature is valid the security de-

vice forwards the message for further proceedings, e.g. to store the message in a database, otherwise the message is rejected.

This method has the drawback, that the content of the message can be modified between the creation of the message and the generation of the signature by the sender as well as between the validation of the signature and the further proceeding by the receiver.

Therefore, the object of the present invention is to provide a method and an apparatus for generating or validating a signature, which is securer against attacks from non-authorized persons without complicating the method and the apparatus.

This object is solved by a method for validating a message with a signature, wherein said method comprises the step of receiving said message with said signature, and the step of carrying out an integrated validation and storing process, wherein said signature is validated based on a validation algorithm and a key and said received message is stored in a database.

According to the present invention a received message is handled in at least two steps. One step is a receiving step and the other step is an integrated step, wherein two processes are combined, namely the validation of the signature and the processing of the message.

In the scope of the present invention, messages are an accumulation of information. A message can be for example a document or a contract. That means the message can be a complete business contract with information about the sender and the receiver or just the content. In a preferred embodiment of the present invention the message is an Extensible Markup Language (XML) document. XML is a universal format for structured documents and data on the Web. The term message can include the signature. In an embodiment of the present invention the

signature can also be transmitted without the signed document. In this case the term message is used for the signature alone.

According to the present invention the message is verified by validating the signature of the message. This signature is a cryptographic means through which the origin of a document and the identity of the sender may be verified. In addition, the signature verifies, that the message has not been changed since the message has been signed by the holder of the signature's private key. The signature is a piece of information based on the document to be signed, a signature algorithm and on a key of the sender. An example for a signature algorithm is the Digital Security Algorithm (DSA) over a hash function.

In a preferred embodiment of the present invention asymmetric keys with a public and a private key are used. The generator of the signature uses his private key and the receiver of the signature uses the public key to verify the sender.

The integrated process of validating the signature and storing the message according to the present invention enables for the first time, that the message cannot be changed between the signature validation and the storing. Only in the case where the signature of the message is valid, this integrated process causes a processable version of the message. Otherwise the message will not enter an area in which validated messages will be processed.

One example to carry out this integrated process is to store the message and to validate the signature within one atomic process. Only in the case that the signature can be validated the storing of the message is completed and the transaction is committed. Otherwise the storing process is rolled back, that means all data, which has already been stored, is deleted. Alternatively, the data of not validated messages can be stored in an insecure area. If the receiver has used the wrong key for the validation, there is no need to submit the complete message again. The

receiver can retrieve the message from the insecure area and carry out the integrated validation and storing process again.

According to a preferred embodiment of the invention the received message is locked before the integrated validation and the storing step is initiated, and until this integrated step is finished. This means that nobody can change anything within the message to be validated during the integrated process and manipulate the result.

The integrated process is preferably carried out in one device and this is preferably the device in which the received message is processed. In the present example the message is stored in a storage device and the method is carried out by the storage device. This inventive realization has the advantage that the complete validation and storing process can be controlled by one person, for example by the administrator of the storage device.

According to a preferred embodiment of the present invention the signature is a digital signature. This digital signature is preferably an XML signature. XML signatures can be applied to any digital content of one or more resources. Different kinds of XML signatures are known in the art. For example, an enveloped signature is generated based on message data within the same XML document and a detached signature is generated based on external data. The different kinds of XML signatures are described in the W3C specification (http://www.w3.org/TR/xmldsig-core/).

In a preferred embodiment of the present invention the integrated validation and storing process is carried out as an ACID (Atomic, Consistent, Isolation and Durable) transaction. This transaction provides a simple model of success or failure. Either the transaction is committed, that means all actions are carried out, or the transactions aborts, that means no action is carried out or all carried out actions are revoked.

The term atomic means that the transaction cannot be divided into smaller parts. The transaction can either be carried out complete or not at all. Consistency in the scope of an ACID transaction defines the transformation of data from one consistent state into another consistent state. Each transaction is isolated, which means, that other transactions, which access the same resources have to be carried out before or after the current transaction is finished. The result of a transaction is durable. ACID transactions are described, for example, in "Transaction processing: Concepts and Techniques" by Jim Gray and Andreas Reuter.

The object of the present invention is also solved by a method for generating a signature for a message that is the result of a database access. Said method comprises the step of carrying out an integrated receiving and generating process, wherein a message to be sent is received, in other words prepared, and a signature is generated based on a signing algorithm and a key and the step of sending the message with the signature.

According to the present invention a message to be sent is handled in at least two steps. One step is an integrated step, wherein two tasks are combined in one process, namely the processing of the message and the generating of the digital signature. In the second step the message is sent.

According to the present invention a signature is generated. This signature is a cryptographic means through which the authenticity of a document and the identity of the signer may be verified. The signature is a piece of information based on the document to be signed, a signature algorithm and on a key of the sender.

The integrated process of receiving the message to be sent and generating the signature guarantees that at no point of time the message can be changed. According to a preferred embodiment of the invention the message can be locked against

access before the integrated step is initiated and until the integrated step is finished.

As already described in connection with the integrated validation and storing process, all tasks are preferably carried out in one transaction. This method guarantees that either both parts of the integrated process succeed or both fail.

The object of the present invention is also solved by a method for validating a message with a signature, wherein said method comprises receiving said message with said signature, starting an ACID transaction, sending a request to a security device, validating said signature in said security device, storing of said message in response to the result of the validation and committing the ACID transaction.

The object of the present invention is also solved by a method for generating a signature for a message, wherein said method comprises starting an ACID transaction, acquiring said message to be signed, sending a request to a security device, generating a signature for said message in said security device, committing said ACID transaction and sending said message with said signature.

The object of the present invention is also solved by an apparatus for validating a message with a signature, wherein said apparatus comprises means for receiving said message with said signature, and means for carrying out an integrated validation and storing process, wherein said means are capable and affected to validate said signature based on a validation algorithm and a key and to store said message.

The object of the present invention is also solved by an apparatus for generating a signature for a message, wherein said apparatus comprises means for carrying out an integrated receiving and generating process, wherein said means are capable and affected to receive said message to be sent and to generate said signature

based on a signing algorithm and a key, and means for sending said message with said signature.

The invention is in the following exemplary described by means of the following drawing, which shows:

Figure 1: A flowchart representing a validation and storing process according to the prior art.

Figure 2: A flowchart representing a receiving and generating process according to the prior art.

Figure 3: A flowchart representing an integrated validation and storing process according to the present invention.

Figure 4: A flowchart representing an integrated receiving and generating process according to the present invention.

Figure 5: A flowchart representing a validation process.

The present invention is now described together with an archive device. This archive device comprises a database where messages, preferably XML-documents, can be stored and retrieved from an external user. The user has access to the archive device via a data network, for example the Internet.

Figure 1 shows the validation and storing process of a message according to the prior art. A client 1 sends a digitally signed message to a receiving device, in this example the archive device 2. The message passes the firewall 3 and arrives at the security device 4 of the archive device 2. At this security device 4 the signature of the message is validated.

If the validation succeeds, the message, which is now a trusted message, is forwarded to a storage device 5 in the archive device 2. The storage device 5 receives the trusted message and stores the trusted message in a database 6. In the present example, the validated signature is also forwarded to the storage device 5 and

stored in the database 6. Now, the storage device 5 can confirm the successful reception of the trusted message to the client 1.

In a prior art system as described in Figure 1 the trusted message could be modified or replaced between the security device 4 and the storage device 5 by a not legitimated person. This enables the not legitimated person to store any trustless message in the database 6 of the storage device 5.

The same problem occurs, when a receiving and generating process is carried out by an archive device 2 according to the prior art. Figure 2 shows such a process. The client 1 sends a request for a message to the storage device 5 in the archive device 2. This request passes the firewall 3. In the storage device 5 the requested message is received from the database 6 and forwarded to the security device 4. In the security device 4 the message is signed and the message is sent together with the signature via the firewall 3 to the client 1.

Again, a not legitimated person could modify or replace the message, i.e. the response between the storage device 5 and the security device 4.

Figure 3 shows how this problem is solved by the present invention. When the client 1 sends a signed message (possibly through a firewall 3) to the archive device 2', the signed message is received by the storage device 5'. The security device 4' according to the present invention is not capable to receive messages. The storage device 5' starts an ACID transaction. Within the ACID transaction the received message and the received signature are locked. That means, that no parallel updates of the message or the signature are allowed while the transaction is running. This achieves, that no other action with the message, the signature or the key is possible as long as integrated validation and storing process is not finished.

After the transaction has been started, the integrated validation and storing process is initiated. One part of this integrated process - namely the validation - is carried

out, in the present example, in the security device 4' of the archive device 2' and the other part - namely the storing - is carried out in the storage device 5' of the archive device 2'. But these two parts are processed within the same transaction, so that an independent modification of one part is not possible.

If the validation succeeds and the verified message has been stored the transaction is committed (and the locks are released). The stored message is now protected by the security of the storage device 5. If the signature validation fails, the storage process is stopped and rolled back and the message may be rejected or stored in another area.

The corresponding method for sending a signed message is illustrated in Figure 4. The client 1 sends a request for a message to the archive device 2'. The request is received by the storage device 5' of the archive device 2'. In response to the request, the storage device 5' initiates, that it receives the requested message, for example from the database 6. According to the present invention the receiving is carried out by the storage device 5' in one ACID transaction as an integrated receiving and generating process. The signature is generated in the security device 4' After the message has been received and signed the signed message is sent to the client 1.

The process of validation is described in more detail in connection with Figure 5. Figure 5 shows a flowchart illustrating the different steps during the validation process. Before the validation process is carried out, the message, in the present example an XML document, is received. Then a transaction is started and it is checked if the document is signed or not. If the message is not signed, the message is stored and the transaction is committed.

If the message is signed, the message is stored and the document is pre-processed into a normalized form according to canonicalization rules. In the present example, the signature comprises two parts. One part comprises references to the

signed documents, nodes, or subnodes, the transform algorithms, which identify the signed parts of the documents and a hash value over the data of the referenced part. The second part of the signature is a hash value over the complete first part of the signature, which is ciphered by the private key of the signer.

In order to validate the first part of the signature, the signed parts of the documents are identified based on the references, the transform algorithms are applied and a hash value is calculated over these parts. If this calculated hash value corresponds to the first hash value in the part of the signature, this part of the validation process was successful.

The ciphered second hash value in the second part of the signature is employed to ensure, that the first hash value has not been modified. For this, a hash value is calculated over the first part of the signature and compared with the second hash value, deciphered with the public key of the signer.

If both parts of the validation process have been successful, the signature is valid and the transaction is committed. Otherwise, the signature is not valid and the complete transaction is rolled back.

Software AG

September 12, 2002
S37957EP JH/Hdt/tge

Claims

1. Method for validating a message with a signature, wherein said method comprises the following steps:
   a) receiving said message with said signature, and
   b) carrying out an integrated validation and storing process, wherein said signature is validated based on a validation algorithm and a key and said received message is stored in a database.

2. Method according to claim 1, wherein in said integrated validation and storing process said message is stored and said signature is validated within one atomic process.

3. Method according to any of claims 1 or 2, wherein the storing process is rolled back, if the signature is not valid.

4. Method according to any of claims 1 to 3, wherein the storing process is completed, if the signature is valid.

5. Method according to any of claims 1 to 4, wherein said received message is locked before the integrated validation and storing process is carried out and released after the integrated validation and storing process has been finished.

6. Method according to any of claims 1 to 5, wherein said received signature is locked before the integrated validation and storing process is carried out and released after the integrated validation and storing process has been finished.

7. Method according to any of claims 1 to 6, wherein the integrated validation and storing process is carried out by said database.

8. Method according to claim 7, wherein the integrated validation and storing process is controlled by said database.

9. Method according to any of claims 1 to 8, wherein said message is an XML-document.

10. Method according to any of claims 1 to 9, wherein said signature is a digital signature.

11. Method according to any of claims 1 to 10, wherein said integrated validation and storing process is carried out as ACID transaction.

12. Method for generating a signature for a message, wherein said method comprises the following steps:
    a) carrying out an integrated receiving and generating process, wherein said message to be sent is received and said signature is generated based on a signing algorithm and a key, and
    b) sending said message with said signature.

13. Method according to claim 12, wherein in said integrated receiving and generating process said message to be sent is received and said signature is generated within one atomic process.

14. Method according to any of claims 12 or 13, wherein said message to be sent is locked before the integrated receiving and generating process is carried out and released after the integrated receiving and generating process has been finished.

15. Method according to any of claims 12 to 14, wherein said key to be used for generating the signature is locked before the integrated receiving and generating process is carried out and released after the integrated receiving and generating process has been finished.

16. Method according to any of claims 12 to 15, wherein said message is an XML-document.

17. Method according to any of claims 12 to 16, wherein said integrated receiving and generating process is carried out as ACID transaction.

18. Method according to any of claims 12 to 17, wherein said integrated receiving and generation process is carried out in a database, where said message to be sent is stored.

19. Method according to any of claims 12 to 18, wherein said signature is a digital signature.

20. Method for validating a message with a signature, wherein said method comprises the following steps:

a) receiving said message with said signature,
b) starting an ACID transaction,
c) sending a request to a security device,
d) validating said signature in said security device,
e) storing of said message in response to the result of the validation, and
f) committing said ACID transaction.

21. Method for generating a signature for a message, wherein said method comprises the following steps:
    a) starting an ACID transaction,
    b) acquiring said message to be signed,
    c) sending a request to a security device,
    d) generating a signature for said message in said security device,
    e) committing said ACID transaction, and
    f) sending said message with said signature.

22. Apparatus for validating a message with a signature, wherein said apparatus comprises:
    - means for receiving said message with said signature, and
    - means for carrying out an integrated validation and storing process, wherein said means are capable and affected to validate said signature based on a validation algorithm and a key and to store said message.

23. Apparatus for generating a signature for a message, wherein said apparatus comprises:
    - means for carrying out an integrated receiving and generating process, wherein said means are capable and affected to receive said message to be sent and to generate said signature based on a signing algorithm and a key, and
    - means for sending said message with said signature.

Software AG

September 12, 2002
S37957EP JH/Hdt/tge

Abstract

Method and apparatus for validating a message with a signature, wherein said method comprises the step of receiving said message with said signature, and carrying out an integrated validation and storing process, wherein said signature is validated based on a validation algorithm and a key and said received message is stored in a database and a method and apparatus for generating a signature for a message, wherein said method comprises the steps of carrying out an integrated receiving and generating process, wherein said message to be sent is received and said signature is generated based on a signing algorithm and a key, and sending said message with said signature.

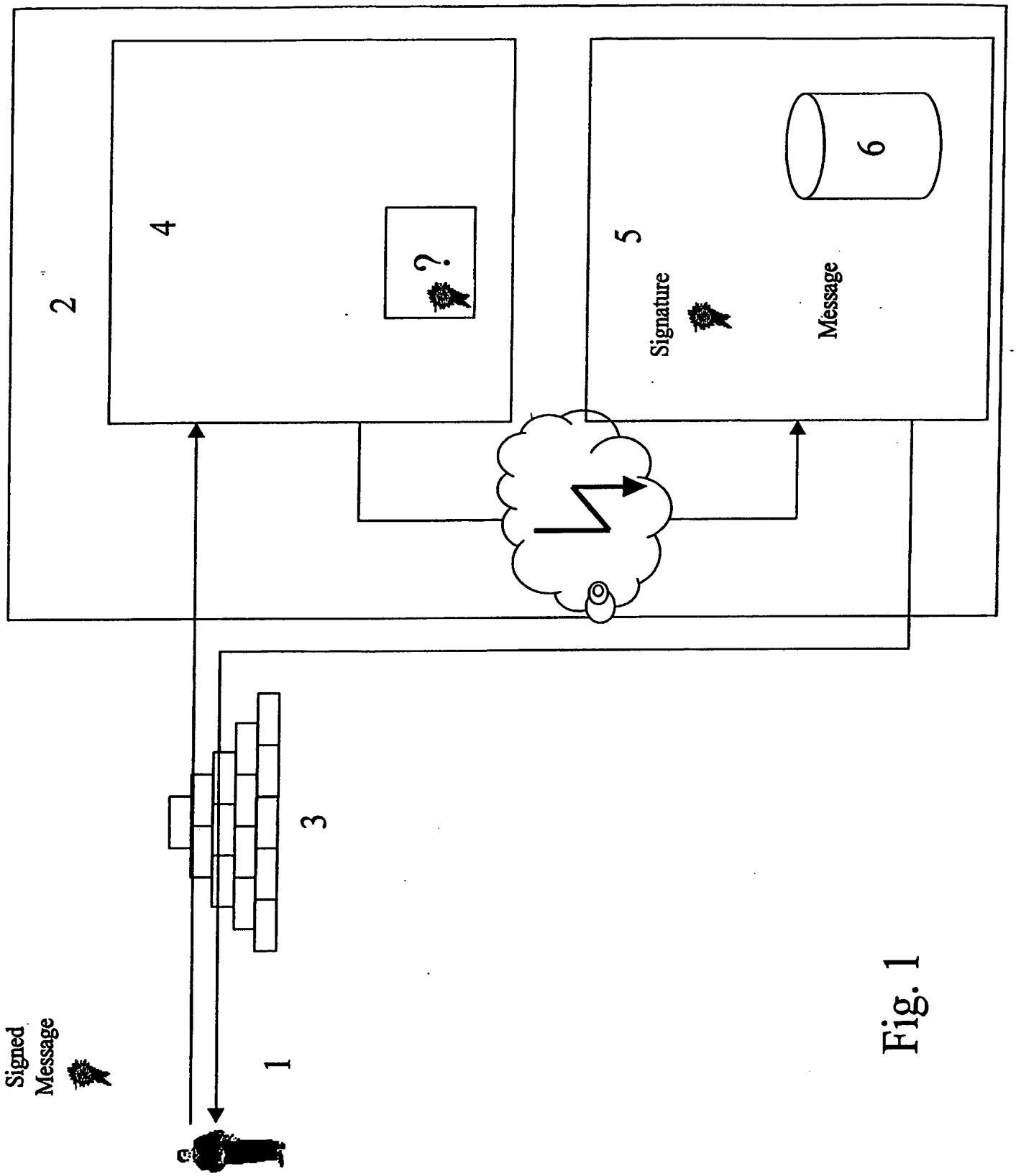

Fig. 1

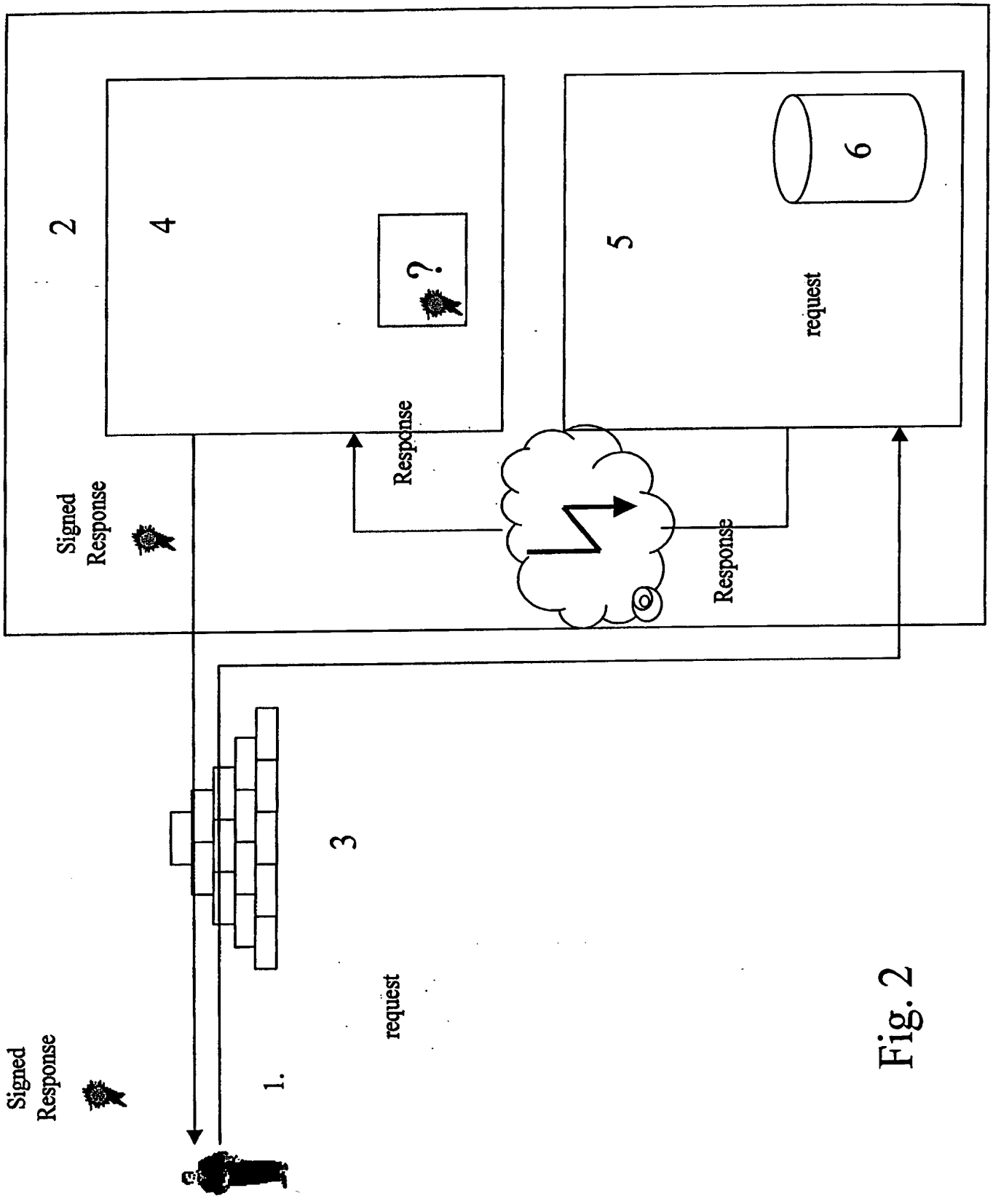
Signed Response
1.
request
3
2
Signed Response
4
?
Response
5
request
6
Response

Fig. 2

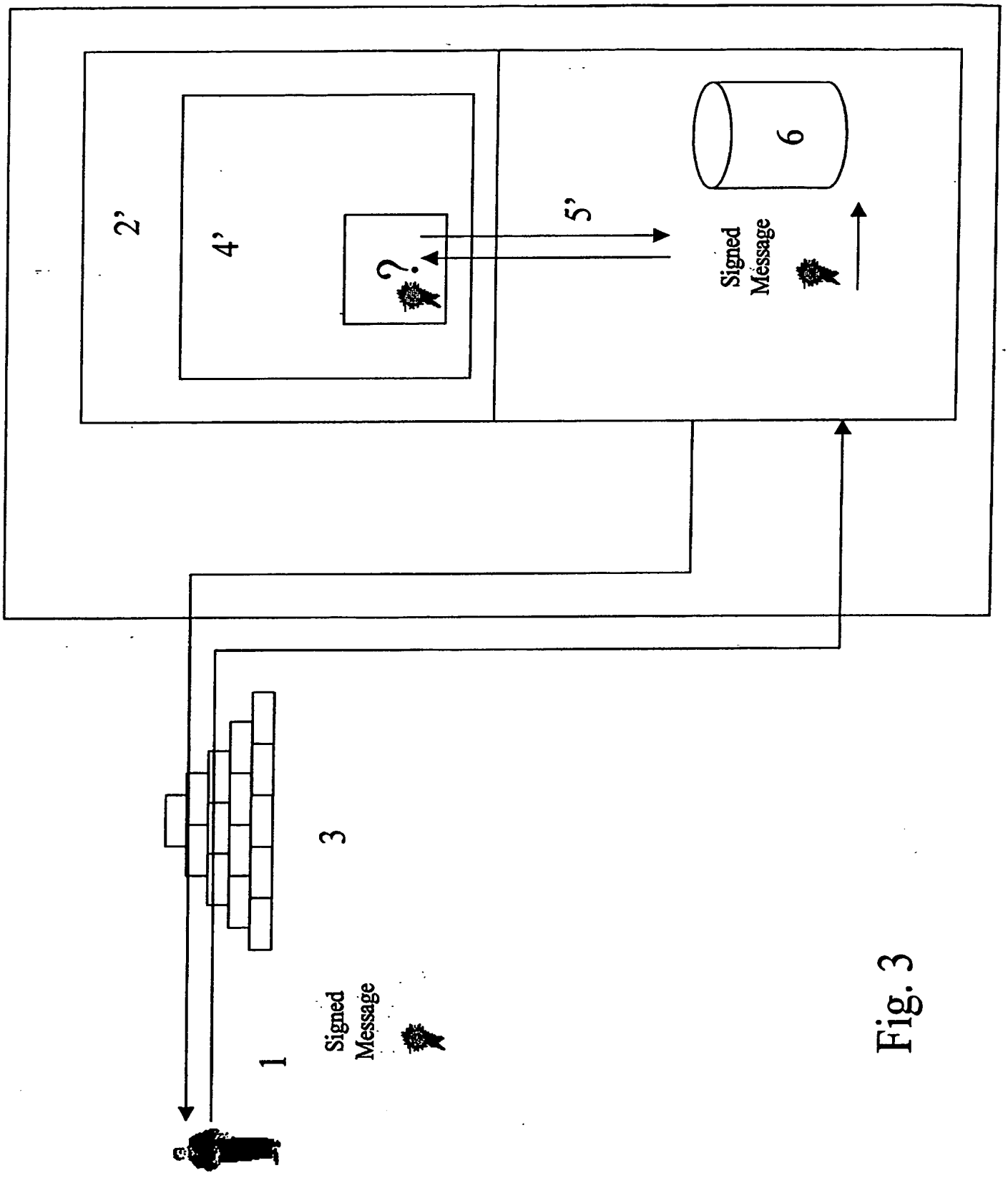

Fig. 3

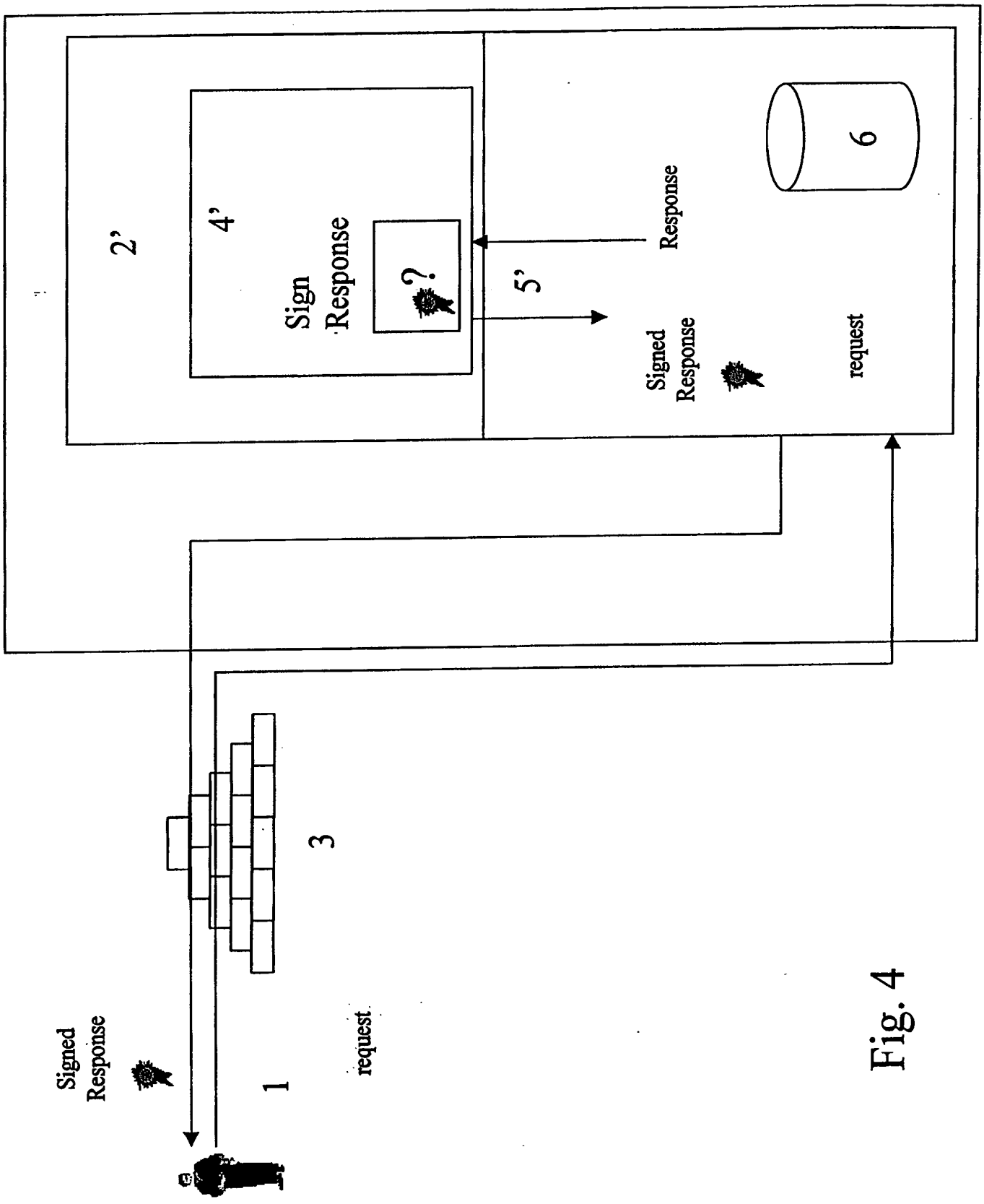
2'
4'
Sign
Response
?
5'
Response
Signed
Response
request
6
Signed
Response
1
request
3

Fig. 4

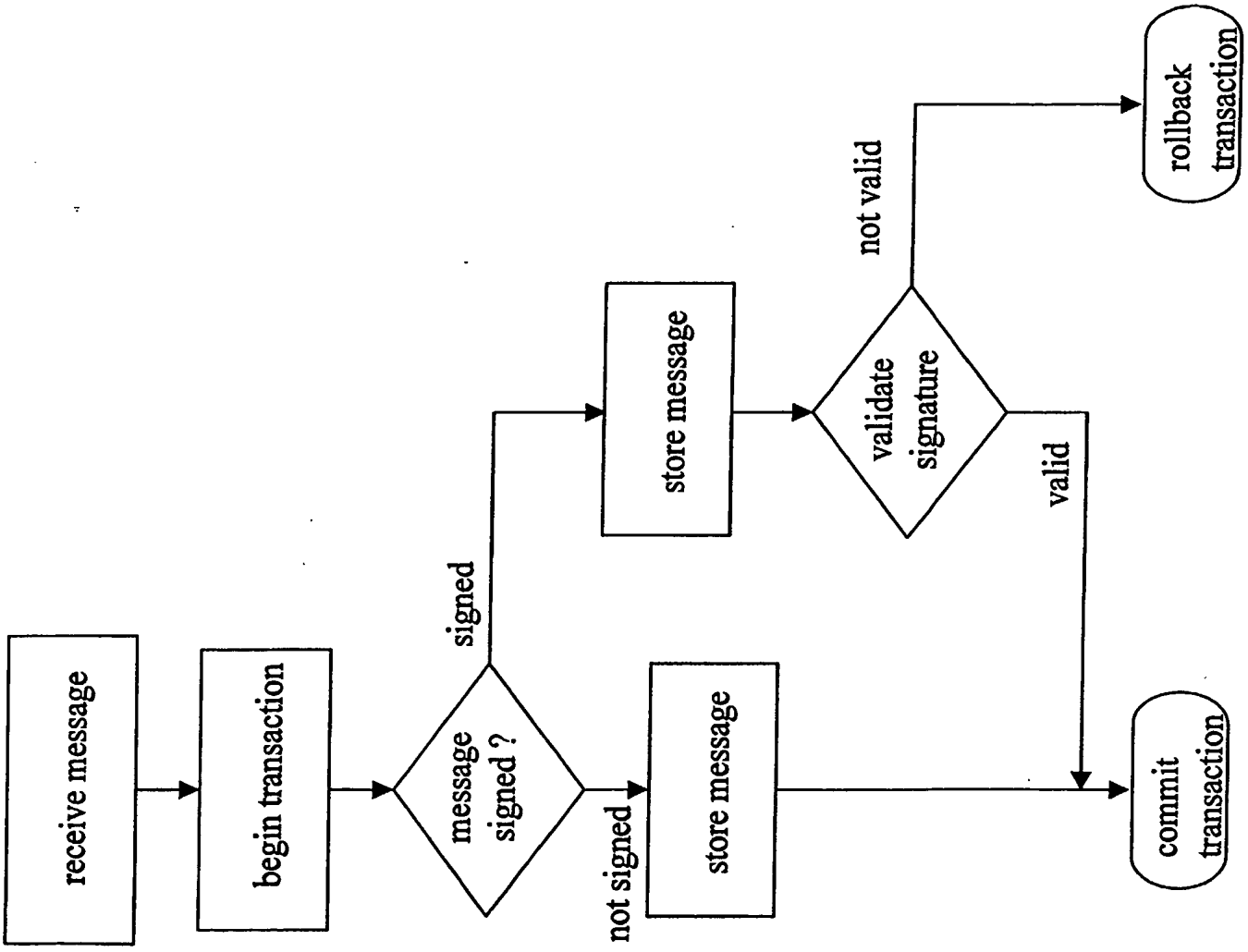
receive message
begin transaction
message signed ?
signed
not signed
store message
store message
validate signature
not valid
valid
rollback transaction
commit transaction

Fig. 5